

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
22 April 2004 (22.04.2004)

PCT

(10) International Publication Number
WO 2004/034673 A1

(51) International Patent Classification?: **H04L 29/06,**
H04Q 7/38

(21) International Application Number:
PCT/GB2003/004315

(22) International Filing Date: 8 October 2003 (08.10.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0223311.2 8 October 2002 (08.10.2002) GB

(71) Applicant (for all designated States except US): **IPWIRE-
LESS, INC.** [US/US]; 1001 Bayhill Drive, 2nd Floor, San
Bruno, CA 94066 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **WILLIAMS, An-
drew, Gordon** [GB/GB]; 79 Ashford Road, Swindon,

Wiltshire SN1 3NT (GB). **PARKER, Andrew** [GB/GB];
195 Monmouth Drive, Sutton Coldfield B73 6JS (GB).

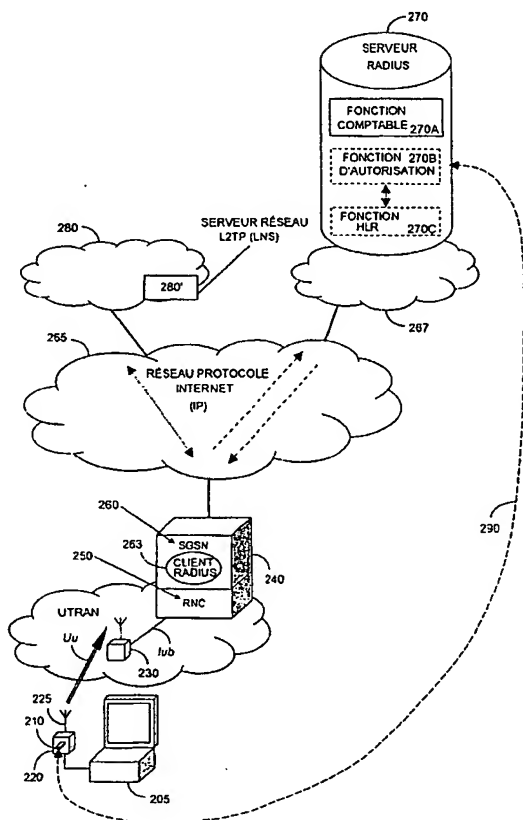
(74) Agent: **HUDSON, Peter**; InetIP, 121 Blackberry Lane,
Four Marks, Alton, Hampshire GU34 5DJ (GB).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,
MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG,
SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN,
YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,
SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: **SYSTEM AND METHOD TO PROVIDE UMTS AND INTERNET AUTHENTICATION**



(57) Abstract: System (FIG. 2) and method for use of internet authentication technology to provide UMTS authentication. An SGSN (260) in an Integrated Network Controller (240) in a UMTS network and a RADIUS server (270) are adapted to support signalling therebetween whereby authentication of a USIM is performed in the RADIUS Server. This allows a conventional Authorisation Centre (AuC) to be replaced by the RADIUS Server, and it is substantially cheaper, because it is based largely on existing off-the-shelf Internet access authentication technology, modified to this purpose.

WO 2004/034673 A1

**Declarations under Rule 4.17:**

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD TO PROVIDE UMTS AND INTERNET AUTHENTICATION**5 Field of the Invention**

This invention relates to Wireless Internet Access systems, and in particular those based on UMTS 3G (Universal Mobile Telecommunication System 3rd Generation) mobile standards.

Background of the Invention

15 The UMTS standards describe a particular method by which an end-user's piece of equipment (UE) is authenticated and also the mechanism by which the UE authenticates the network (to prevent it connecting to bogus base stations). These require particular signalling from the SGSN (Serving General Packet Radio Service Support Node) element to a UMTS HLR/AuC (Home Location Register / Authentication Centre). This is covered in the following standards documents:

- 25 [1] TS 33.102 - 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture; (Release 1999), and
- 30 [2] TS 24.008 - 3rd Generation Partnership Project; Technical Specification Group Core Network;

- 2 -

Mobile radio interface layer 3 specification;
Core Network Protocols - Stage 3; (Release
1999).

5 The standards also recommend an algorithm set for such
authentication functions:

- 10 [3] TS 35.205 - 3rd Generation Partnership Project;
Technical Specification Group Services and
System Aspects; 3G Security; Specification of
the MILENAGE Algorithm Set: An example
algorithm set for the 3GPP authentication and
key generation functions f1, f1*, f2, f3, f4,
f5 and f5*; Document 1: General (Release 4),
15 and
- [4] TS 35.206 - 3rd Generation Partnership Project;
Technical Specification Group Services and
System Aspects; 3G Security; Specification of
the MILENAGE Algorithm Set: An example
20 algorithm set for the 3GPP authentication and
key generation functions f1, f1*, f2, f3, f4,
f5 and f5*; Document 2: Algorithm Specification
(Release 4).

25 However, this known approach has the disadvantage(s) that
due to the complexity of the existing standards and the
relatively small market for such elements it is expensive
to implement, and generally based on bespoke software,
and in some cases bespoke hardware.

30

- 3 -

From patent publication no. WO 02/11467 there is known use of RADIUS (Remote Authentication Dial-In User Service) and associated protocols to authenticate network access for fixed end users and for end users who roam in a wireless system. RADIUS is standardized by the IETF (Internet Engineering Task Force) in the document:

[5] RFC 2865 - Remote Authentication Dial In User Service.

10 The standards documents [1]-[5] referred to above are hereby incorporated herein by reference.

However, this known use of RADIUS supports authentication for end users using UE associated with a computer such as a PC (Personal Computer). It does not facilitate support of USIM (UMTS Subscriber Identify Module) cards in UE.

A need therefore exists for use of internet authentication technology to provide UMTS authentication services related to USIMs wherein the abovementioned disadvantage(s) may be alleviated.

Statement of Invention

25

In accordance with the present invention there is provided a system and a method for use of internet authentication technology to provide UMTS authentication as claimed in claim 1 and claim 15 respectively.

30

- 4 -

Brief Description of the Drawings

One system and method use of internet authentication technology to provide UMTS authentication services related to UMTS SIM cards (USIMs) incorporating the present invention will now be described, by way of example only, with reference to the accompanying drawing(s), in which:

10 FIG. 1 shows a block schematic diagram illustrating signal sequencing in a prior art system to authenticate a user;

15 FIG. 2 shows a block schematic diagram of a UTRAN Internet system illustrating the present invention;

20 FIG. 3 shows a block schematic diagram illustrating signal sequencing during normal authentication process in the system of FIG. 2; and

25 FIG. 4 shows a block schematic diagram illustrating signal sequencing during anti-replay data synchronisation process in the system of FIG. 2.

Description of Preferred Embodiment(s)

The UMTS standards describe a particular method by which an end-user's piece of equipment (UE) is authenticated and also the mechanism by which the UE authenticates the network (to prevent it connecting to bogus base

30

- 5 -

stations). These require particular signalling from the SGSN element to a UMTS Home Location Register / Authentication Centre (HLR/AuC). This is covered in the standards documents [1], [2], [3] & [4] referred to
5 above.

As shown in FIG. 1, the method of the UMTS standards utilises the network elements USIM 110, UE 120, Node B 130, RNC 140, SGSN 150, HLR 160 and AuC 170. The
10 authentication-related signalling effectively occurs between the USIM 110, SGSN 150 and AuC 170.

The AuC 160 generates a set of authentication and keying material, called an Authentication Vector; sets of
15 Authentication Vectors are sent to the SGSN 150 by the AuC 170, at the request of the SGSN.

The authentication of a UE 120 occurs when it 'attaches' to the network:
20 On an attempted network attach from a UE 120, the SGSN 150 selects an existing Authentication Vector, or requests fresh Authentication Vectors from the AuC 170. The SGSN then supplies the random challenge value (RAND) and the Authentication Token (AUTN) values from the
25 Authentication Vector to the USIM 110.

The USIM uses a shared secret value (shared with the AuC) referred to as K, plus any other parameters demanded by the authentication algorithm (the UMTS standards supply
30 an example algorithm called MILENAGE, which has the values OP - Operator Variant Configuration Field - and

- 6 -

AMF - Authentication Management Field) to authenticate the network by validating the AUTN value it received. The authentication algorithm also includes a scheme to prevent replay-attacks (where a sequence of authentication messages is recorded, then re-played at a later time, in order to gain un-authorized access to a service) based on synchronised changing values in the AuC to the USIM (in the MILENAGE algorithm this is achieved using a changing sequence number shared between USIM and AuC, referred to as SQN).

If the USIM authenticates the network successfully, it generates an authentication result value (RES) and sends it back to the SGSN.

The SGSN compares RES against XRES and if they match authentication completes and the UE is allowed onto the network.

When the USIM authenticates the network, it can detect out-of-synchronisation anti-replay-attack data between it and the AuC - in this case a re-synchronisation procedure is executed between the USIM and AuC and the authentication procedure is then re-executed.

As will be described in greater detail below, in its preferred embodiment the present invention is based on an Internet technology-based authentication server, using a commercial RADIUS authentication server platform, that implements the procedures such that:

- 7 -

- the SGSN function within an Integrated Network Controller (INC - comprising RNC and SGSN functionality) can obtain the required authentication and keying material to authenticate a
5 UE containing a USIM; and
- the network authentication function within the USIM can authenticate the INC.

As described in the present applicant's co-pending patent
10 application no. US 09-432,824 (published in equivalent form as EP 1098539) and co-pending patent application no. GB 0114813.9, the contents of which applications are hereby incorporated herein by reference, a combined RNC/SGSN may be supported in a single network element.
15 In this configuration the function of the HLR and AuC can be replaced with a RADIUS based Internet authentication server, as described in the present applicant's co-pending patent application no. US 09-626,700 (published in equivalent form as WO 02/11467), the content of which
20 is hereby incorporated herein by reference.

The present invention is based on the realisation by the inventors that the earlier-described use of RADIUS to authenticate the UE for wireless access, can be extended
25 by extensive modification of the signalling procedures to support the use of USIM cards in the UE. The signalling required to implement this in detail below.

The RADIUS protocol allows for vendor-specific extensions
30 to messages. Commercial RADIUS server software also supports the addition of software functionality ('plug-

- 8 -

in') to process/create RADIUS messages, including attributes added as extensions to the RADIUS protocol. The present invention is based on the realisation by the inventors that the functionality of the UMTS AuC, and the associated signalling with the SGSN, can be replaced by extensions to the RADIUS protocol and a software 'plug-in' on the RADIUS server.

Referring now to FIG. 2, a wireless access user of the Internet access system has a PC (Personal Computer) 205 and UMTS user equipment (UE) 220 containing a USIM card 210. The UE has a directly attached antenna 225 and is connected by typical wired data connection such as RS232, USB or Ethernet to the PC 205. The UE 220 and USIM 210 are together commonly termed a mobile terminal, operating in conjunction with the associated PC 205 (which is commonly termed terminal equipment).

The UE 220 communicates over a wireless link *Uu* with a base station or Node B 230 in an access network domain of a UTRAN network. The Node B 230 communicates over a link *Iub* with an integrated network controller (INC) 240. As discussed above, the INC 240 includes an RNC (Radio Network Controller) 250, which controls and allocates the radio network resources and provides reliable delivery of user traffic between the Node B 230 and the UE 220, and an SGSN (Serving General Packet Radio Service Support Node) 260, which provides session control. The SGSN 260 incorporates a RADIUS element designated RADIUS client 263 to provide authentication and other functions, as will be described in greater detail below.

- 9 -

The INC 240 is connected to an Internet protocol network 265 and then to a UMTS access network operator 267, having a RADIUS server 270. The RADIUS server 270
5 incorporates RADIUS Accounting Functions 270A, and Authentication Functions 270B and HLR Functions 270C (these functions are shown in dashed line in FIG. 2 because, as will be described in greater detail below, the functionality is provided in software in the RADIUS
10 Server, rather than by provision of a dedicated AuC and HLR as previously known). The RADIUS server 270 is the server for both authentication and accounting functions. Thus, after authentication normally the user would communicate via the network 265 with target Internet
15 service provider 280 through its Layer 2 Tunneling Protocol Network Server LNS 280'.

As will be explained in greater detail below, a link 290 is effectively established between the USIM 210 and
20 authentication functionality 270B within the RADIUS server 270, allowing authentication of the USIM 210 without requiring a dedicated authentication centre and a dedicated home location register.

25 The RADIUS Server 270:

- Is provisioned with the IMSI-derived User-Name derived from the numeric IMSI identifier within the USIM (e.g., for an IMSI value of 234151234567890 the RADIUS User-Name attribute might be
30 "234151234567890_attach") and also the set of security parameters required to support generation

- 10 -

of the various parts of a UMTS Authentication Vector.

- Has had its RADIUS attribute dictionary extended, to include a 'UMTS-Authentication-Vector' attribute, containing RAND, AUTN, CK, IK and XRES with the same functionality (size in bits) as the values defined in UMTS standards document [3] referred to above.
- Has its RADIUS attribute dictionary extended, to include a 'UMTS-Resynchronisation-Token' attribute, containing a value with the same definition as the AUTS parameter described in UMTS standards document [3] referred to above.
- Has a software plug-in that supports generation of a UMTS-Authentication-Vector RADIUS attribute, based on the provisioned security parameters and the dynamic anti-replay parameters.
- Has a software plug-in that supports re-synchronisation of the dynamic anti-replay parameters with the USIM, on reception of a UMTS-Resynchronisation-Token attribute.

Referring now also to FIG. 3, the normal authentication process is as follows:

- 310 - The UE 220 initiates the attach procedure.
- 320 - The SGSN module 260 within the INC 240 requests a single Authentication vector, via a RADIUS Access-Request message; the RADIUS User-Name attribute (see the IETF standards document [5] referred to above) contains a RADIUS user ID

- 11 -

derived from the numeric IMSI identifier within the USIM (e.g., for the IMSI value "0123456789012345" the User-Name attribute would contain the value:
5 "0123456789012345_attach").

The RADIUS server plug-in derives a UMTS-Authentication-Vector attribute (made up of: RAND, AUTN, XRES, CK and IK values) based on
10 the provisioned information and the dynamic anti-replay-attack information. The attribute is returned to the SGSN module 260 within the INC 240 in an Access-Accept RADIUS message.

15 330 - The USIM 210 authenticates the network, using RAND and AUTN values received from the SGSN, then generates an authentication result value (RES) and sends it back to the SGSN module 260 within the INC 240.

20 340 - The SGSN module 260 within the INC 240 compares RES against XRES and if they match authentication completes and the UE 220 is allowed onto the network.

25 The following table describes how the RADIUS Access-Request message and the RADIUS Access-Accept message can be constructed:

- 12 -

Message	Contained Attribute	Type / Value	Notes
Access-Request	User-Name	Octet string	IMSI from SIM card with "_attach" appended to it
	User-Password	Octet string	Default value inserted by INC
	NAS-IP-Address	IP Address	
	User-Name-Type	Enumerated value	Identifies whether the User-Name value represents an IMSI
Access-Accept	Vendor-Specific (UMTS-Authentication-Vector)	Octet String	72-76 Byte concatenation of authentication material as defined in 3GPP specifications

The Octet String of the RADIUS Access-Accept message is constructed as shown in the following table:

Octets			
0	1	2	3
Type	Length	Vendor-ID	
Vendor-ID (continued)		Manuf.-Type	Manuf.-Length
RAND (128 bit)			
CK (128 bit)			
IK (128 bit)			
AUTN (128 bit)			
XRES (64-128 bit)			

5

The 'Type' field has a vendor-specific value (e.g., 26).

The 'Length' field has a typical value of 80.

The 'Vendor-ID' field has the vendor's IANA-assigned value (e.g., 5586).

- 10 The 'Manuf.-Type' (Manufacturer-Type) field has the UMTS-Authentication-Vector value of 14.

- 13 -

The 'Manuf.-Length' field has a value in the range 74 - 78.

The Value field (RAND, CK, IK, AUTN and XRES) is 72 - 76 octets of concatenated authentication material to be used
5 by the INC in Access Authentication, challenge and ciphering.

Referring now also to FIG. 4, the anti-replay data synchronisation process is as follows:

10

410 - The UE 220 initiates the attach procedure.

15

420 - The SGSN module 260 within the INC 240 requests a single Authentication vector, via a RADIUS Access-Request message; the RADIUS User-Name attribute (see the IETF standards document [5] referred to above) contains a RADIUS user ID derived from the numeric IMSI identifier within the USIM (e.g., for an IMSI value of
20 234151234567890 the RADIUS User-Name attribute might be "234151234567890_attach").

25

The RADIUS server plug-in derives a UMTS-Authentication-Vector attribute (made up of: RAND, AUTN, XRES, CK and IK values) based on the provisioned information and the dynamic anti-replay-attack information. The attribute is returned to the SGSN module 260 within the INC 240 in an Access-Accept RADIUS message.

30

- 14 -

430 - The USIM 210 authenticates the network, using
RAND and AUTN values received from the SGSN
260, and it detects that the anti-replay-attack
data is out of synchronisation, but all other
5 data is correct. The USIM 210 sends a message
to the SGSN 260 containing the value AUTS (see
the UMTS standards document [2] referred to
above), signifying that the anti-replay attack
data is out of date.

10

440 - In this case the USIM initiates the re-
synchronisation procedure.

450 - The SGSN module 260 within the INC 240 requests
15 a single Authentication vector, via a RADIUS
Access-Request message; this message also
includes the UMTS AUTS value in a UMTS-
Resynchronisation-Token RADIUS attribute, which
contains a hidden version of its anti-replay-
20 attack information from the USIM.

The RADIUS server plug-in re-synchronises the
anti-replay attack information, then derives a
UMTS-Authentication-Vector attribute based on
25 the provisioned information and the now back-
in-sync dynamic anti-replay information. The
UMTS-Authentication-Vector attribute is
returned to the SGSN module 260 within the INC
240 in an Access-Accept RADIUS message.

30

- 15 -

460 - The USIM authenticates the network, using RAND
and AUTN values received from the SGSN 260,
then generates an authentication result value
(RES) and sends it back to the SGSN module
5 within the INC.

470 - The SGSN module within the INC compares RES
against XRES and if they match authentication
completes and the UE is allowed onto the
10 network.

The message sent from the USIM 210 to the SGSN 260 at
step 430 above, signifying that the anti-replat-attack
data is out of date, is constructed as shown in the
15 following table:

Octets			
0	1	2	3
Type	Length	Vendor-ID	
Vendor-ID (continued)		Manuf.-Type	Manuf.-Length
AUTS (112 bit)			

The 'Type' field has a vendor-specific value (e.g., 26).
The 'Length' field has a typical value of 22.
20 The 'Vendor-ID' field has the vendor's IANA-assigned
value (e.g., 5586).

- 16 -

The 'Type' field has the UMTS-Resynchronisation-Token value of 15.

The 'Manuf.-Length' field has a value of 16.

The Value field (AUTS) is 14 octets of concatenated
5 authentication material to be used by the RADIUS server
270 in USIM sequence number resynchronisation.

It will be understood that by extending the signalling
procedures as described above, RADIUS may be used to
10 authenticate a USIM card in a UE for wireless access in a
UMTS system, by effectively establishing a link between
the USIM and authentication functionality within the
RADIUS server (as shown by the link 290 in FIG. 2)
without requiring a dedicated authentication centre (and
15 a dedicated home location register).

It will be appreciated that the method described above
for use of internet authentication technology to provide
UMTS authentication may be carried out in software
20 running on one or more processors (not shown) in the
RADIUS server 270, the SGSN module 260 and the PC
carrying the USIM 210, and that the software may be
provided as a computer program element carried on any
suitable data carrier (also not shown) such as a magnetic
25 or optical computer disc.

It will be understood that the use of internet
authentication technology to provide UMTS authentication
services related to UMTS SIM cards (USIMs) described
30 above provides the following advantages:

- 17 -

- it is substantially cheaper than prior art solutions, because
- it is based largely on existing off-the-shelf Internet access authentication technology, modified
5 (conveniently in software in the USIM, SGSN and/or RADIUS server) to this purpose.

- 18 -

Claims

1. A system for use of internet authentication technology to provide UMTS authentication, the system
5 comprising:
Serving GPRS Support Node (SGSN) means in a UMTS network; and
RADIUS server means,
the SGSN means and the RADIUS Server means being adapted
10 to support signalling therebetween whereby authentication of a User Subscriber Identity Module (USIM) may be performed in the RADIUS Server means.
2. The system of claim 1 wherein the SGSN means is
15 integrated with Radio Network Controller (RNC) means in Integrated Network Controller (INC) means.
3. The system of claim 1 or 2 wherein the UMTS network comprises a UMTS Terrestrial Radio Access Network (UTRAN).
20
4. The system of any preceding claim wherein the SGSN means is adapted to send an Access-Request RADIUS message to request a UMTS Authentication Vector from the RADIUS server means.
25
5. The system of any preceding claim wherein the RADIUS Server means is adapted to generate authentication and keying material so as to authenticate a USIM within a UMTS UE, according to UMTS standards.
30

- 19 -

6. The system of claim 5 wherein the RADIUS Server means is adapted to implement the MILENAGE algorithm.
7. The system of claim 5 or 6 wherein the RADIUS Server means is adapted to generate, using anti-replay-attack dynamic data, a UMTS Authentication Vector, for use by the SGSN means.
8. The system of claim 5 when dependent on claim 4 wherein the RADIUS Server means is adapted to support dynamic sequence number (SQN).
9. The system of any preceding claim wherein the RADIUS Server means is adapted to generate a UMTS Authentication Vector in a RADIUS attribute within an Access-Accept RADIUS message for sending to the SGSN means.
10. The system of any preceding claim wherein the SGSN means is adapted to receive a UMTS Authentication Vector in a RADIUS Access-Accept message.
11. The system of any preceding claim wherein the SGSN means is adapted to send information to re-synchronise anti-replay-attack information within the USIM with the RADIUS Server means.
12. The system of claim 11 when dependent on claim 4 wherein SGSN means is adapted to send a UMTS-Resynchronisation-Token attribute in the Access-Request RADIUS message.

- 20 -

13. The system of claim 12 wherein the RADIUS Server means is adapted to reset anti-replay-attack dynamic data in-line with the USIM in response to the data received in the UMTS-Resynchronisation-Token.

5

14. The system of claim 13 wherein the RADIUS Server means is adapted to implement the MILENAGE algorithm.

15. A method for use of internet authentication technology to provide UMTS authentication, the method comprising:

providing Serving GPRS Support Node (SGSN) means in a UMTS network; and

providing RADIUS server means,

15 signalling between the SGSN means and the RADIUS Server means so that authentication of a User Subscriber Identity Module (USIM) is performed in the RADIUS Server means.

20 16. The method of claim 15 wherein the SGSN means is integrated with Radio Network Controller (RNC) means in Integrated Network Controller (INC) means.

17. The method of claim 15 or 16 wherein the UMTS network comprises a UMTS Terrestrial Radio Access Network (UTRAN).

18. The method of any one of claims 15-17 wherein the SGSN means sends an Access-Request RADIUS message to request a UMTS Authentication Vector from the RADIUS server means.

30

- 21 -

19. The method of any one of claims 15-18 wherein the
RADIUS Server means generate authentication and keying
material so as to authenticate a USIM within a UMTS UE,
5 according to UMTS standards.

20. The method of claim 19 wherein the RADIUS Server
means implements the MILENAGE algorithm.

10 21. The method of claim 19 or 20 wherein the RADIUS
Server means generates, using anti-replay-attack dynamic
data, a UMTS Authentication Vector and sends the it to
the SGSN means.

15 22. The method of claim 19 when dependent on claim 18
wherein the RADIUS Server means supports dynamic sequence
number (SQN).

20 23. The method of any one of claims 15-22 wherein the
RADIUS Server means generates a UMTS Authentication
Vector in a RADIUS attribute within an Access-Accept
RADIUS message and sends it to the SGSN means.

24. The method of any one of claims 15-23 wherein the
25 SGSN means receive a UMTS Authentication Vector in a
RADIUS Access-Accept message.

25. The method of any one of claims 15-24 wherein the
SGSN means sends information to re-synchronise anti-
30 replay-attack information within the USIM with the RADIUS
Server means.

- 22 -

26. The method of claim 25 when dependent on claim 18 wherein the SGSN means sends a UMTS-Resynchronisation-Token attribute in the Access-Request RADIUS message.

5

27. The method of claim 26 wherein the RADIUS Server means resets anti-replay-attack dynamic data in-line with the USIM in response to the data received in the UMTS-Resynchronisation-Token.

10

28. The method of claim 27 wherein the RADIUS Server means implement the MILENAGE algorithm.

29. A RADIUS Server adapted to perform the method of any one of claims 15-28.

15

30. A SGSN adapted to perform the method of any one of claims 15-28.

31. A computer program element comprising computer program means for performing the method of any one of claims 15-28.

20

1/4

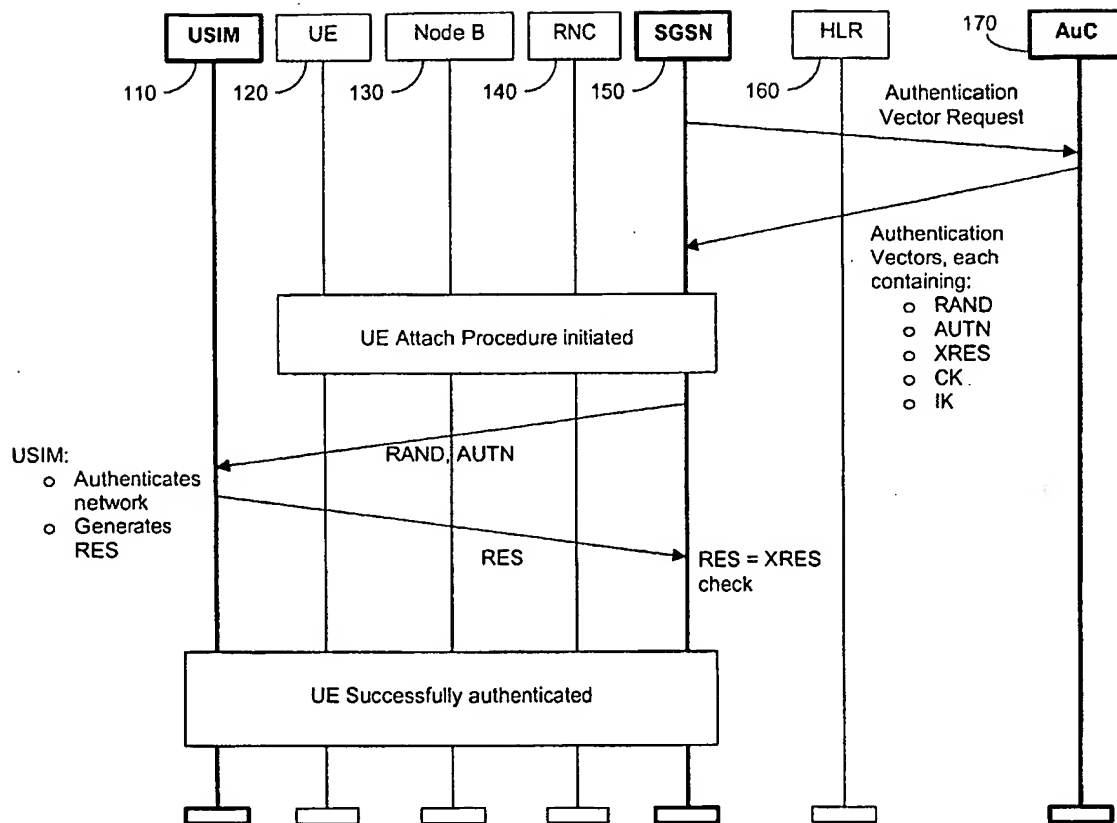
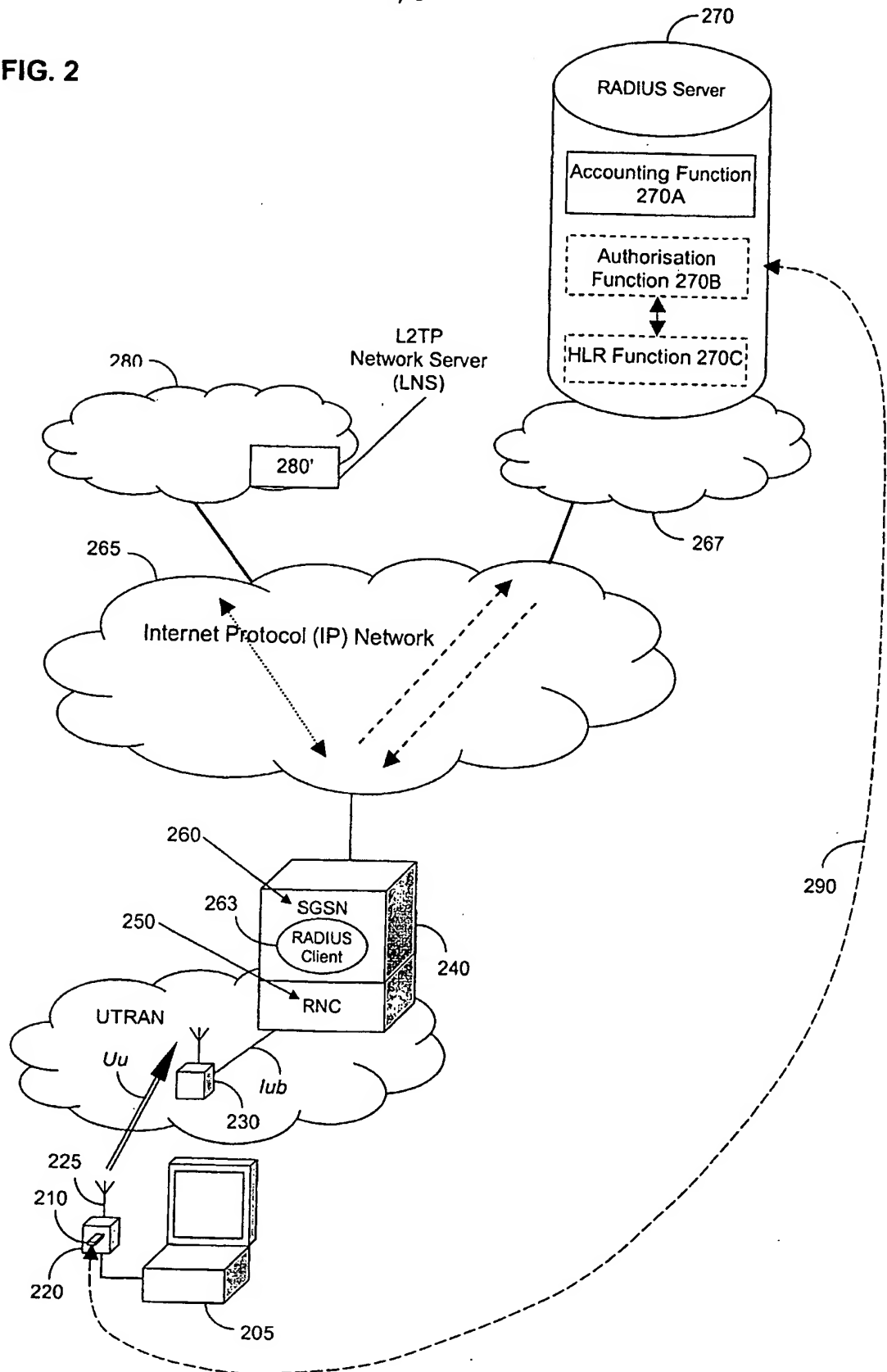


FIG. 1
Prior Art

2/4

FIG. 2



3/4

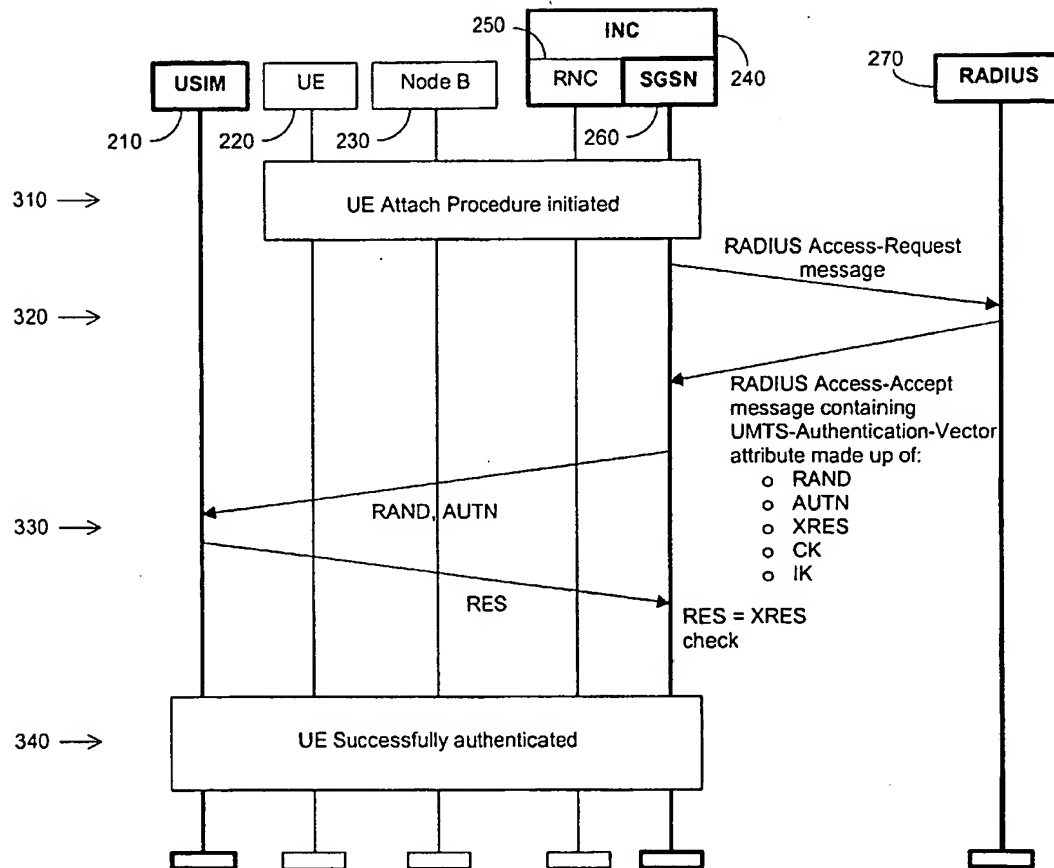


FIG. 3

4 / 4

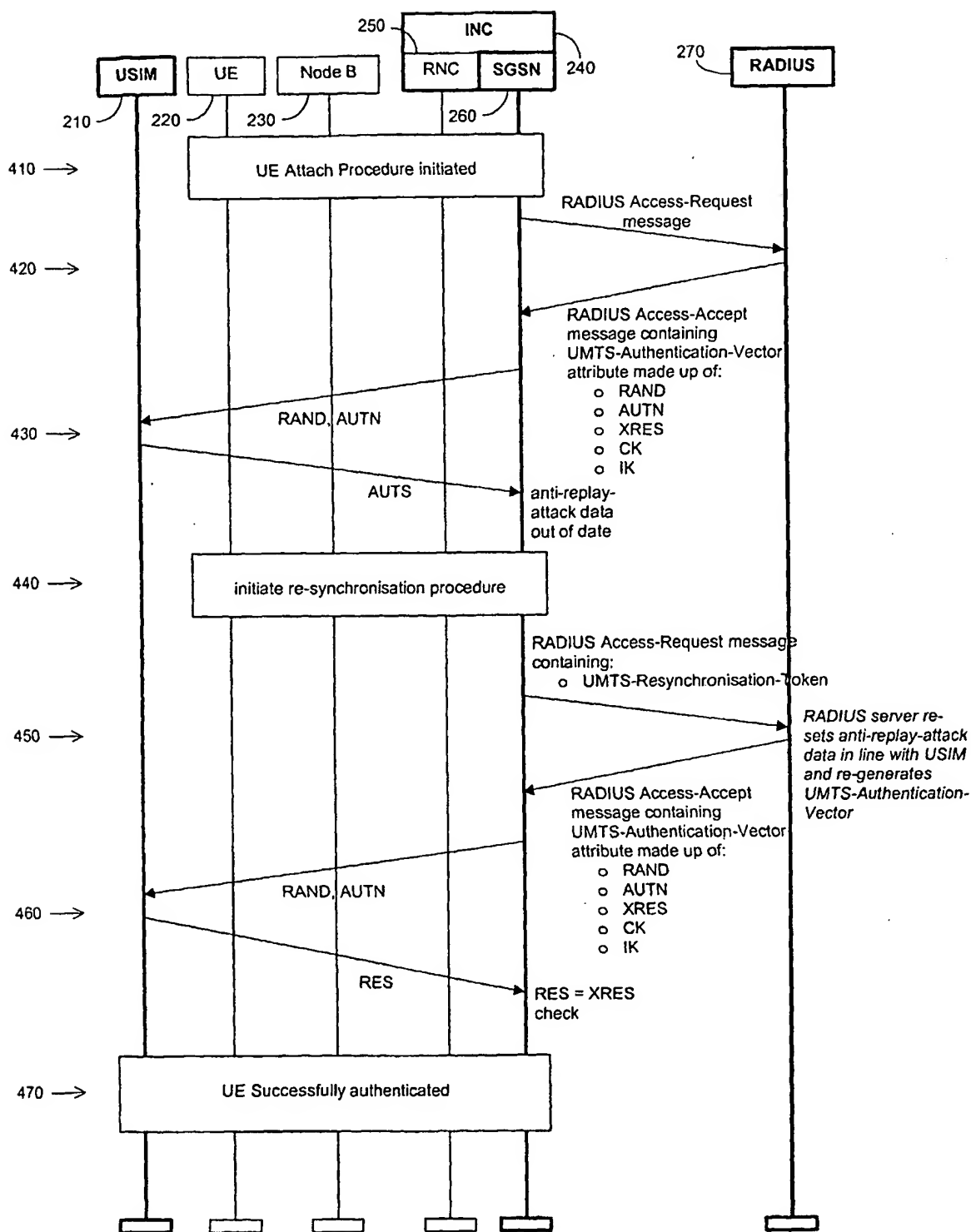


FIG. 4

INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 03/04315

A. CLASSIFICATION OF SUBJECT MATTER
 IPC 7 H04L29/06 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, PAJ, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 02 11467 A (BOWRING MICHAEL ; JONES WILLIAM JOHN (GB); WILLIAMS ANDREW GORDON () 7 February 2002 (2002-02-07) cited in the application the whole document	1-31
Y	WO 01 76297 A (NOKIA MOBILE PHONES LTD ; RINNEMAA JYRI (FI); EKBERG JAN ERIK (FI);) 11 October 2001 (2001-10-11) page 1, line 11 -page 2, line 19 page 6, line 9 -page 7, line 10 page 9, line 12 -page 10, line 24 page 21, line 29 -page 23, line 6 page 24, line 30 -page 25, line 12 figures 1,2	1-31



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

Z document member of the same patent family

Date of the actual completion of the international search

16 February 2004

Date of mailing of the international search report

24/02/2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax: (+31-70) 340-3016

Authorized officer

Carnerero Álvaro, F

INTERNATIONAL SEARCH REPORT

Internat ☐ Application No

PCT/GB 03/04315

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	<p>HAVERINEN H ET AL: "CELLULAR ACCESS CONTROL AND CHARGING FOR MOBILE OPERATOR WIRELESS LOCAL AREA NETWORKS" IEEE WIRELESS COMMUNICATIONS, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 9, no. 6, December 2002 (2002-12), pages 52-60, XP001143468 ISSN: 1070-9916 page 54, right-hand column -page 55, left-hand column; figure 3 -----</p>	1-31

INTERNATIONAL SEARCH REPORT

Internat Application No

PCT/GB 03/04315

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 0211467	A	07-02-2002	CA 2384890 A1	07-02-2002
			WO 0211467 A2	07-02-2002
			GB 2369271 A	22-05-2002
<hr/>				
WO 0176297	A	11-10-2001	AU 5043901 A	15-10-2001
			EP 1273197 A1	08-01-2003
			WO 0176297 A1	11-10-2001
			US 2003157926 A1	21-08-2003
<hr/>				